The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/15/2016

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP which could allow an attacker to potentially execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting these issues may allow remote attackers to execute arbitrary code in the context of a webserver.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. There is known proof-of-concept code for these vulnerabilities.

SYSTEM AFFECTED:
- PHP 7.0 prior to 7.0.4
- PHP 5.0 prior to 5.6.19
- PHP 5.0 prior to 5.5.33

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
PHP has released updates that address multiple vulnerabilities that could allow for arbitrary code execution. These vulnerabilities include:

Prior to 7.0.4

- Bug 71450 (An integer overflow in php_str_to_str_ex()).
- Bug 71637 (Multiple Heap Overflow due to integer overflows in xml/filter_url/addcslashes).

Successful exploitation of these vulnerabilities may allow remote attackers to execute arbitrary code in the context of the webserver. Other bugs fixed in PHP for these versions may be found below:

- Bug 71441 (Typehinted Generator with return in try/finally crashes).
- Bug 71442 (forward_static_call crash).
- Bug 71443 (Segfault using built-in webserver with intl using symfony).
- Bug 71449 (An integer overflow in php_implode()).
- Bug 71474 (Crash because of VM stack corruption on Magento2).
- Bug 71485 (Return typehint on internal func causes Fatal error when it throws exception).
- Bug 71529 (Variable references on array elements don't work when using count).
- Bug 71601 (finally block not executed after yield from).

Prior to 5.5.33

- Bug 71498 (Out-of-Bound Read in phar_parse_zipfile()).

Prior to 5.6.19

- Bug 62172 (FPM not working with Apache httpd 2.4 balancer/fcgi setup).
- Bug 68078 (Datetime comparisons ignore microseconds).
- Bug 70720 (strip_tags improper php code parsing).
- Bug 71434 (finfo throws notice for specific python file).
- Bug 71498 (Out-of-Bound Read in phar_parse_zipfile()).
- Bug 71523 (Copied handle with new option CURLOPT_HTTPHEADER crashes while curl_multi_exec).
- Bug 71525 (Calls to date_modify will mutate timelib_rel_time, causing date_date_set issues).
- Bug 71540 (NULL pointer dereference in xsl_ext_function_php()).
- Bug 71559 (Built-in HTTP server, we can download file in web by Bug).
- Bug 71561 (NULL pointer dereference in Zip::ExtractTo).
- Bug 71584 (Possible use-after-free of ZCG(cwd) in Zend Opcache).

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

PHP:
http://php.net/ChangeLog-5.php#5.5.33
http://php.net/ChangeLog-5.php#5.6.19

http://php.net/ChangeLog-7.php#7.0.4

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/